

Algebra Qual Studying

Kat Shultis

April 11, 2010

Contents

1	Group Theory	3
1.1	Previous Material	3
1.2	Class Equation	3
1.3	Group Actions	3
1.4	Sylow's Theorems	4
1.5	Representation on Cosets	4
1.6	Construction of New Groups	4
1.7	Solvable, Nilpotent and Simple Groups	5
1.8	Normal Series	6
1.9	Fundamental Theorem of Finite Abelian Groups	6
2	Field and Galois Theory	8
2.1	Field Extensions	8
2.2	Galois Theory	9
2.3	Splitting Fields	10
2.4	Simple Extensions	11
2.5	Finite Fields	11
2.6	Algebraic Closure	11
2.7	Radical Extensions	12
2.8	Irreducibility	12
2.9	Cyclotomic Polynomials	12
2.10	Algebraic (In)dependence	13
3	Rings and Modules	14
3.1	Definitions	14
3.1.1	Ring specific Definitions	14
3.1.2	Module specific Definitions	15
3.1.3	Definitions connecting Rings and Modules	16
3.1.4	Definitions involving Groups, Rings, and/or Fields	17
3.2	Theorems and Other Ring/Module Statements	17

3.2.1	Integral Domains	17
3.2.2	Chain Conditions, Noetherian, Artinian	18
3.2.3	Modules over a PID	19
3.2.4	Exact Sequences	19
3.2.5	Semiprime Artinian Rings	19
3.2.6	Nilpotence	20
3.2.7	Algebraic Geometry Introduction	21
3.2.8	Division Rings	21
3.2.9	Tensor Products	21
3.2.10	Vector Spaces, Matrices, and Linear Transformations	22
3.2.11	Simple Rings and Modules	23
3.2.12	Prime, Primitive and Maximal: Rings, Ideals, and Elements	23
3.2.13	Group Algebras	24
3.2.14	Miscellaneous	24

1 Group Theory

1.1 Previous Material

Proposition. *The cosets of a normal subgroup, $N \triangleleft G$, partition G .*

Remark. If $N \triangleleft G$ and $H \subset G$, then $NH := \{nh : n \in N, h \in H\}$ is a subgroup of G , and

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|}.$$

Definition. The **normalizer** of a subgroup $H \subset G$ is the set $N_G(H) := \{g \in G : gHg^{-1} \subset H\}$.

Remark. $N_G(H)$ is the largest subgroup of G in which H is normal.

Definition. An **inner automorphism** of a group G is of the form $x \mapsto gxg^{-1}$.

Proposition. *For $n \geq 3$, A_n is generated by the 3-cycles.*

1.2 Class Equation

Definition. The **conjugacy class** of an element $a \in G$ is the set $\text{cl}(a) := \{g^{-1}ag : g \in G\}$.

Proposition. *The conjugacy classes of two elements are either disjoint, or the same.*

Proposition. *The number of elements in a conjugacy class of a is the same as the index of the centralizer of a .*

Theorem. *The **class equation** is*

$$|G| = |Z(G)| + \sum_{a \in G \setminus Z(G)} |\text{cl}(a)|.$$

Definition. A **p-group** is a group of order p^n for some prime p and $n \geq 1$.

Theorem. *The center of a p-group is nontrivial.*

Cauchy's Theorem. *If a prime, p , divides the order of a group, G , then G has an element of order p .*

1.3 Group Actions

Definition. A group G **acts on** a set X if there is a map $\phi : G \rightarrow A(X)$ where $A(X)$ is the set of all one-to-one mappings of X onto itself.

Definition. For a group G acting on a set X , the **orbit of x** is the set of all elements of X that x can be sent to under the group action, that is, $\mathcal{O}(x) := \{gx = \phi(g)(x) : g \in G\}$.

Definition. The **stabilizer of x** is the set of elements of G that fix x , that is $\text{st}(x) := \{g : gx = x\}$.

Proposition. *The orbits partition the set X . That is, two orbits are either equal or disjoint, and every element in X is in some orbit.*

Proposition. *For a group G acting on a set X , the number of elements in the orbit of x is the index of the stabilizer of x in G .*

Corollary. *If G is a finite group, then the number of elements in the stabilizer of x divides the order of G .*

1.4 Sylow's Theorems

Definition. Let G be a finite group, with $|G| = p^m t$, and $(p, t) = 1$. Then a **p -Sylow subgroup of G** is a subgroup of order p^m .

Sylow's 1st Theorem. *For every $p|O(G)$, then G has a p -Sylow subgroup.*

Lemma. *If P is a p -Sylow subgroup of G , then P is the unique p -Sylow subgroup of $N_G(P)$.*

Sylow's 2nd Theorem. *Any two p -Sylow subgroups are conjugate.*

Corollary. *A p -Sylow is normal in G if and only if it is unique.*

Sylow's 3rd Theorem. *If G is a finite group, and $p|O(G)$, then the number of p -Sylow subgroups in G is of the form $1 + kp$, with $k \in \mathbb{N}$, and the number of p -Sylow subgroups must divide the order of the group.*

Lemma. *If G is any finite group, and P is a p -Sylow subgroup of G , then $N_G(N_G(P)) = N_G(P)$.*

1.5 Representation on Cosets

Theorem. *Let $H \subset G$ be a subgroup of finite index, $i_G(H)$. Then there exists a homomorphism $\phi : G \rightarrow S_{i_G(H)}$ with kernel a subgroup of H .*

Corollary. *If G is a finite group and $O(G) \nmid i_G(H)!$, then H contains a nontrivial normal subgroup of G .*

1.6 Construction of New Groups

Definition. An **external direct product** of groups H_1, \dots, H_n is $H_1 \times \dots \times H_n := \{(h_1, \dots, h_n) : h_i \in H_i\} = (e)$ with multiplication defined componentwise.

Proposition. *If $N_1, \dots, N_t \triangleleft G$, $N_1 N_2 \dots N_t = G$, and $N_i \cap (N_1 \dots \widehat{N_i} \dots N_t) = \{e\}$ for all i , then $G \cong N_1 \times \dots \times N_t$.*

Corollary. *An abelian group is the external direct product of its Sylow subgroups.*

Theorem. *If G is abelian, and for $x \in G$, the equation $x^n = e$ has at most n solutions in G , then G is cyclic.*

Corollary. *If G is a finite multiplicative subgroup of a field, then G is cyclic.*

1.7 Solvable, Nilpotent and Simple Groups

Definition. The **commutator subgroup** of G is the subgroup generated by all **commutators**, $a^{-1}b^{-1}ab$, and is denoted $[G, G]$. The **i^{th} derived subgroup** of G is $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$. In general, the commutator subgroup $[K, L] = \langle k^{-1}l^{-1}kl : k \in K, l \in L \rangle$ and $K, L \subset G$.

Definition. A group G is **solvable** if $G^{(n)} = (e)$ for some n .

Definition. A subgroup of a group is called **characteristic** if for any automorphism, ϕ , of G , then $\phi(H) \subset H$.

Remark. $[G, G]$ is characteristic in G .

Proposition. *If $N \triangleleft G$, then G/N is abelian if and only if $H \supset [G, G]$.*

Theorem. *Every subgroup and every homomorphic image of a solvable group is solvable.*

Theorem. *If $N \triangleleft G$, with N and G/N both solvable, then G is solvable.*

Definition. The **descending central series** of G is $\gamma_1(G) \supset \gamma_2(G) \supset \dots$ where $\gamma_1(G) := G$ and $\gamma_i := [G, \gamma_{i-1}(G)]$.

Definition. The **ascending central series** of G is $Z^0(G) \subset Z^1(G) \subset \dots$ where $Z^0(G) = (e)$, and $Z^i(G)$ is the inverse image of the center of $G/Z^i(G)$. Here, $Z^i(G)$ is called the **i^{th} higher center** of G . Note that $Z^1(G) = Z(G)$ is the center of G .

Theorem. *$Z^m(G) = G$ if and only if $\gamma_{m+1}(G) = (e)$.*

Definition. A group is **nilpotent** if the equivalent conditions in the above theorem hold.

Theorem. *Every subgroup and every homomorphic image of a nilpotent group is nilpotent.*

Theorem. *A direct product of nilpotent groups is nilpotent.*

Proposition. *Any p -group is nilpotent.*

Corollary. *A direct product of p -groups is nilpotent.*

Remark. $A_3 \triangleleft S_3$, A_3 is nilpotent, as is $S_3/A_3 \cong \mathbb{Z}_2$, but S_3 is not nilpotent.

Theorem. *A finite group is nilpotent if and only if it is a direct product of its Sylow subgroups.*

Theorem. *Every nilpotent group is solvable.*

Lemma. *If $N \subset Z(G)$ and G/N is nilpotent, then G is nilpotent.*

Lemma. *If the subgroup $U \subset S_n$ with $n > 4$ contains every 3-cycle and if $N \triangleleft U$ is such that U/N is abelian, then N contains every 3-cycle.*

Lemma. *If G is nilpotent, and $H \subset G$, then $N_G(H) \supsetneq H$.*

Theorem. *S_n is not solvable for $n > 4$*

Corollary. *A_5 is simple.*

Theorem. *A_n is simple for $n \geq 5$.*

1.8 Normal Series

Definition. A **normal series** of G is a chain of subgroups $G = G_0 \supset G_1 \supset \dots \supset G_t = (e)$ such that $G_i \triangleleft G$. If the restriction that $G_i \triangleleft G$ is loosened to be that $G_i \triangleleft G_{i+1}$, then this is called a **subnormal series**. The factor groups, G_i/G_{i+1} , are called **subquotients**. The **length** of the series is t .

Definition. A **refinement** of a normal series is one that is obtained by the insertion of additional subgroups. We also allow for a normal series to be a refinement of itself.

Definition. A normal series is called a **composition series** if G_i/G_{i+1} is simple for all i .

Definition. Two normal series are **equivalent** if there exists a one-to-one correspondence between factor groups such that the corresponding factor groups are isomorphic.

Schreier Refinement Theorem. *Two normal series of an arbitrary group have equivalent refinements.*

Jordan Holder Theorem. *Any two composition series of a group are equivalent.*

1.9 Fundamental Theorem of Finite Abelian Groups

Lemma. *Every abelian group can be written as the direct sum of p -groups.*

Lemma. *Every finite abelian p -group is a direct sum of cyclic p -groups.*

Theorem. *Let G be a finite abelian group, then G can be written uniquely (up to isomorphism) as: $G = C_1 \oplus \dots \oplus C_n$ with $|C_{i+1}| \mid |C_i|$ and each C_i is a cyclic group.*

Definition. In the above theorem, if $C_i = \mathbb{Z}_{n_i}$, then the n_i s are called the **invariant factors** of G .

Definition. DESCRIBE ELEMENTARY DIVISORS HERE!!

Lemma. *Let G is a finite abelian group, and $|G| = p^n$ with p prime. If G has a unique subgroup of order p , then G is cyclic.*

Lemma. *If C is a cyclic subgroup of maximal order, then $G = C \oplus B$ for some B .*

2 Field and Galois Theory

2.1 Field Extensions

Definition. An element $a \in L$ is **algebraic** over K if there exists a nonzero polynomial $p(x) \in K[x]$ such that $p(a) = 0$. Otherwise, a is said to be **transcendental**.

Remark. A ring generated by a set S over the field K is denoted $K[S]$. The field generated in the same way is denoted $K(S)$.

Definition. A field extension L over K is **algebraic** if every element in L is algebraic over K .

Theorem. Let K be a field, and M a field extension of K . Then if $u \in M$ is algebraic over K and f is a monic polynomial of least degree (say n) with coefficients in K and $f(u) = 0$, then

1. f is unique
2. f is irreducible
3. $1, u, u^2, \dots, u^{n-1}$ form a vector space basis for $K(u)$ over K
4. $[K(u) : K] = n$
5. If $g(x) \in K[x]$ and $g(u) = 0$, then $f(x) | g(x)$.

Theorem. Let $L \supset K \supset F$ be fields, then $[L : F] = [L : K][K : F]$.

Proposition. If $[K : F] \leq n$ then every element in K is algebraic and satisfies a polynomial of degree $\leq n$.

Proposition. $u \in M$ is algebraic over K if and only if $[K(u) : K] < \infty$.

Proposition. If $K(u)$ is infinite dimensional, then $K[u] = K[x]$.

Theorem. If $[L : K] < \text{card}(K)$, then L is algebraic over K .

Proposition. If L is algebraic over K and K is algebraic over F , then L is algebraic over F .

Proposition. If $a, b \in M$ are both algebraic over K , then $a \pm b$ and ab are both algebraic over K . If we also have that $b \neq 0$, then b^{-1} is algebraic over K .

Luroth's Theorem. If $K(x)$ is purely transcendental over K , then any intermediate field will also be purely transcendental.

Weak Nullstellensatz. If K is a field, and $L = K[a_1, \dots, a_n]$ is an extension field, then L is finite dimensional over K .

Lang's Theorem. *Let K be an uncountable field with extension field L . If L is of countable dimension as a vector space over K , then L is algebraic over K .*

Corollary. *If K is an uncountable field, and $K[a_1, \dots, a_n]$ is a field, then $K[a_1, \dots, a_n]$ is finite dimensional over K .*

Proposition. *If $K = Z[a_1, \dots, a_n]$ is a field, with $Z = \mathbb{Z}$ or $Z = \mathbb{Z}_p$, then K is finite.*

2.2 Galois Theory

Definition. The **Galois group of M/K** , denoted $G(M/K)$ is the group of automorphisms, σ of M such that $\sigma|_K = \text{id}$.

Definition. Given fields $M \supset L \supset K$, then $L' := \{\sigma \in G(M/K) | \sigma|_L = \text{id}\} = G(M/L)$.

Definition. Given a Galois group $G(M/K)$ with subgroup H , $H' := \{m \in M | \sigma(m) = m \forall \sigma \in H\}$.

Definition. The field M is **Galois/Normal** over K if $G' = K$.

Proposition. *M is Galois over K if and only if for every $u \in M \setminus K$, there exists a $\sigma \in G$ such that $\sigma(u) \neq u$.*

Proposition. *For fields $M \supset L$, $M' \subset L'$, and $L'' \supset L$. For subgroups, $J \subset H$, $H' \subset J'$, and $H'' \supset H$.*

Definition. An object that is equal to its double prime is called **closed**.

Proposition. *Any primed object is closed.*

Proposition. *For N/K fields, and $G = G(N/K)$, the priming operation sets up a one-to-one inclusion reversing correspondence between closed subgroups of G and closed intermediate fields of N and K .*

Theorem. *If $[M : K] = n < \infty$ as fields, then $[L' : M'] \leq n$. If $[H : J] = n < \infty$, as subgroups of a Galois group, then $[J' : H'] \leq n$.*

Fundamental Theorem of Galois Theory. *Let $N \supset M \supset L \supset K$ be fields with L closed and $[M : L] < \infty$. Then M is also closed, and $[L' : M'] = [M : L]$.*

Similarly, given a Galois group G with subgroups $H \subset J$, then if H is closed and $[J : H] < \infty$, then $[J : H] = [H' : J']$.

Definition. An intermediate field L is called **stable** if every $\sigma \in G(M/K)$ sends L into itself (i.e. $\sigma(L) = L$)

Theorem. *If L is a stable intermediate field, then $L' \triangleleft G = G(M/K)$. Conversely, for a normal subgroup $H \triangleleft G$, we have that H' is a stable intermediate field.*

Corollary. *The closure of a stable intermediate field is stable. The closure of a normal subgroup is normal.*

Theorem. *If $M \supset L \supset K$ are fields and L is Galois and algebraic over K , then L is stable over K .*

Theorem. *If M/K is Galois and $f(x) \in K[x]$ is irreducible with $u \in M$ such that $f(u) = 0$, then f splits completely into distinct linear factors over M .*

Theorem. *If $G(M/K) = G$ and L is a stable intermediate field, then G/L' is isomorphic to the group of all automorphisms of L/K that are extendable to M/K .*

2.3 Splitting Fields

Definition. Given a nonzero polynomial $f(x) \in K[x]$, a field $M \supset K$ is said to be a **splitting field** of f over K if $f(x)$ factors into linear factors over M , and $M = K(u_1, \dots, u_t)$ where the u_i 's are the roots of f . In other words, M is the minimal field in which all of the roots of f exist.

Theorem. *Splitting fields exist and are unique.*

Proposition. *Alternate characterization of splitting fields: If L is a splitting field of f and g is an irreducible polynomial in $K[x]$ that has one root in L , then all of the roots of g are in L .*

Proposition. *If $f(x) \in K[x]$ is irreducible, then there exists a field $K_0 \supset K$ such that K_0 contains a root of f .*

Proposition. *Let K, K_0 be isomorphic fields, with isomorphism ϕ . Then for corresponding polynomials $f(x)$ and $f_0(x)$, we have that $f(x) = \sum a_i x^i \mapsto f_0(x) = \sum \phi(a_i) x^i$.*

Theorem. *For $f(x) \in K[x]$ and $a \in K$, then $(x-a)^2 | f$ if and only if $(x-a) | f$ and $(x-a) | f'$*

Theorem. *Let $f(x)$ be an irreducible polynomial in $K[x]$. Then TFAE:*

1. *In every splitting field $f(x)$ splits into distinct linear factors.*
2. *In some splitting field $f(x)$ splits into distinct linear factors.*
3. *$f'(x) \neq 0$*

Definition. If the conditions in the previous theorem hold for an irreducible polynomial, f , then we say that f is **separable**. An element a is separable if its irreducible polynomial is separable. $M \supset K$ is separable if every element in M is separable and algebraic over K .

Theorem. *Let $[M : K] < \infty$. TFAE:*

1. *M is Galois over K*

2. M is separable over K and M is a splitting field

3. M is the splitting field of a polynomial whose factors are separable.

Theorem. Let $[L : K] < \infty$. Then there exists an $M \supset L$ such that M is a splitting field and if L is separable over K , then M is Galois over K .

Definition. Let $f(x) \in K[x]$. The **Galois group of $f(x)$** is the Galois group of the splitting field of f over K .

2.4 Simple Extensions

Definition. An extension, $L \supset K$ is called **simple** if $[L : K] < \infty$ and there is a $u \in L$ such that $L = K(u)$.

Definition. For a simple extension, $K(u)$, we say that u is a **primitive element**.

Theorem. If $M \supset K$ and $[M : K] < \infty$, then M is simple if and only if there are a finite number of intermediate fields between M and K .

Theorem. If $M \supset K$, and M is finite dimensional and separable over K , then $M = K(u)$ for some u .

Theorem. Every polynomial with real or complex coefficients factors completely into linear factors over \mathbb{C} .

2.5 Finite Fields

Proposition. If K is a finite field, then $\text{char}(K) = p > 0$.

Theorem. A field K has p^n elements if and only if it is the splitting field of $x^{p^n} - x$ over \mathbb{Z}_p .

Corollary. Fields of p^n elements are unique.

Theorem. If $K \subset L$ are finite fields, then L is Galois over K and the Galois group is cyclic.

2.6 Algebraic Closure

Definition. \bar{K} is called the **algebraic closure** of K if \bar{K} is algebraic over K , and every polynomial in $K[x]$ factors completely into linear terms in $\bar{K}[x]$. We say that a field K is algebraically closed if $\bar{K} = K$.

Proposition. Every field has an algebraic closure, and that algebraic closure must be an infinite field.

2.7 Radical Extensions

Definition. A field extension $L \supset K$ is called a radical extension if $L = K(u_1, \dots, u_n)$ where some power of u_i lies in $K(u_1, \dots, u_{i-1})$.

Remark. By inserting additional terms, we can assume that each u_i falls into $K(u_1, \dots, u_{i-1})$ by a prime power.

Theorem. For fields of characteristic 0, $K \subset L \subset M$. If M is a radical extension of K , then $G(L/K)$ is solvable.

Lemma. The composite of radical extensions is radical.

Lemma. In characteristic 0, if L is a radical extension over K , then the Galois closure/normal closure/split closure is also radical.

Lemma. In characteristic 0, if L is a splitting field of $x^n - 1$ over K , then $G(L/K)$ is abelian.

Lemma. If K is a splitting field of $x^n - 1$, and for $a \in K$, L is a splitting field of $x^n - a$, then $G(L/K)$ is abelian.

Definition. $f(x) \in K[x]$ is solvable by radicals if the splitting field of $f(x)$ over K is contained in some radical extension.

Theorem. An equation $f(x) = 0$ is solvable by radicals if its Galois group is solvable.

2.8 Irreducibility

Gauss' Lemma. If $p \in \mathbb{Z}[x]$ is irreducible, then $p \in \mathbb{Q}[x]$ is also irreducible.

Eisenstein's Theorem. Let $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there is a prime such that $p \nmid a_n$, $p \mid a_{n-1}, \dots, a_0$, and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Q}[x]$.

Theorem. If p is prime, and $f(x)$ is irreducible of degree p . Then if we assume that $f(x)$ has exactly two nonreal roots, then the Galois group of $f(x) \in \mathbb{Q}[x]$ is S_p .

2.9 Cyclotomic Polynomials

Definition. A primitive n^{th} root of unity is a root of unity that generates the cyclic group of the n^{th} roots.

Definition. The n^{th} cyclotomic polynomial is of the form $\Phi_n(x) = \prod(x - \theta)$ where each θ is a primitive n^{th} root of unity.

Theorem. $\Phi_m(x)$ is irreducible over \mathbb{Q} for all m .

2.10 Algebraic (In)dependence

Definition. If K is a field and L is an extension field, then $\{y_1, \dots, y_n\} \subset L$ are **algebraically independent** if $f(y_1, \dots, y_n) = 0$ and $f \in K[x_1, \dots, x_n]$ imply that $f = 0$.

Remark. An infinite set is algebraically independent if every finite subset is algebraically independent.

Definition. Let L be a field, and K a subfield of L . If S is a subset of L , then $a \in L$ is **algebraically dependent on S** if a is algebraic over $K(S)$.

Proposition. A nonempty set S is algebraically dependent over K if and only if there is an $a \in S$ which is algebraically dependent over K on $S \setminus \{a\}$

Definition. Given a field L , a subfield K , and a subset of L , say S , then we call $<$ a **dependence relation** if the following hold

- \sim If $a \in S$, then $a < S$.
- \sim If $a < S$, then $a < F$ with F a finite subset of S .
- \sim If $b < S$, and for every $a \in S$, we have that $a < T$, then $b < T$.
- \sim If $a < S$, and $a \not< S \setminus \{b\}$ for some $b \in S$, then $b < (S \cup \{a\}) \setminus \{b\}$.

Proposition. Algebraic dependence is a dependence relation.

Definition. A subset S of the field L with subfield K is a **transcendence basis** if S is algebraically independent, and L is algebraic over $K(S)$.

Theorem. Transcendence bases exist for the field L over K . Also, the cardinality of two such bases is always the same.

3 Rings and Modules

3.1 Definitions

3.1.1 Ring specific Definitions

- ~ The **annihilator** of $a \in R$ is $\text{Ann}(a) = \{r \in R : ra = 0\}$.
- ~ A **principal ideal domain (PID)** is a ring R such that every ideal $I \triangleleft R$ is of the form $I = rR = \{rs : s \in R\} = (r)$.
- ~ A **unique factorization domain (UFD)** is an integral domain such that if $r \in R$, then $r = p_1 \dots p_n$ with p_i primes and this representation is unique up to order and associates.
- ~ An ideal $P \triangleleft R$ is called **prime** if for ideals A, B we have that $AB \subset P$, then $A \subset P$ or $B \subset P$.
- ~ R is a **prime ring** if $I, K \triangleleft R$ are two sided ideals and $IK = (0)$ means that $I = (0)$ or $K = (0)$.
- ~ A ring R is **semiprime** if R has no nonzero nilpotent ideals.
- ~ An ideal P is prime (resp. semiprime), if R/P is prime (resp. semiprime).
- ~ An element r in a ring is called **irreducible** if $r = ab$ means that a or b is a unit. The element is called **prime** if pR is a prime ideal. Lastly, a and b are called **associates** if $a = ub$ for some unit u .
- ~ A ring R is **simple** if $R^2 \neq 0$ and R has no proper two sided ideals.
- ~ In a commutative ring, $x \in R$ is **nilpotent** if $x^n = 0$ for some n . If $x^n = 0$, but $x^{n-1} \neq 0$, then n is the **degree of nilpotence**.
- ~ An element, e , is an **idempotent** if $e^2 = e$.
- ~ The **Jacobson Radical**, $J(R) = \bigcap_{i \in I} M_i$ where $\{M_i\}_{i \in I}$ is the set of all maximal ideals.
- ~ An ideal $I \triangleleft K[x_1, \dots, x_n]$ **vanishes at** (a_1, \dots, a_n) with $a_i \in K$ if $g(a_1, \dots, a_n) = 0$ for all $g \in I$.
- ~ Let K be an algebraically closed field, and let S be a subset of $K[x_1, \dots, x_n]$. Then the **variety determined by** S is $V(S) := \{(e_1, \dots, e_n) \in K^n : f(e_1, \dots, e_n) = 0 \forall f \in S\}$.
- ~ If $Y \subset K^n$, then the **ideal generated by** Y is $I(Y) := \{f \in K[x_1, \dots, x_n] : f(y) = 0 \forall y \in Y\}$.
- ~ $\text{End}_R(M) = \{f : M \rightarrow M \mid f \text{ is a linear, } R\text{-module homomorphism}\}$ is called the **ring of endomorphisms** or the **commuting ring**.

- ~ Given a commutative ring R and another ring S such that there is a ring homomorphism from R into the center of S , then S is a left and right R -module, and we say that S is an **R -algebra**.
- ~ $\bigoplus_{i \in I} M_i$ is all I tuples, but with the restriction that all but finitely many entries are zero. Similarly, $\prod M_i$ is all I tuples with no restriction.

3.1.2 Module specific Definitions

- ~ A **right module** over R is an abelian group $(M, +)$ such that there is an action of R on M written mr such that the following hold:

- $(m_1 \pm m_2)r = m_1r \pm m_2r$,
- $m(r_1 \pm r_2) = mr_1 \pm mr_2$,
- $m(r_1r_2) = (mr_1)r_2$, and
- $m1 = m$ for all $m \in M$.

This module is usually denoted M_R . A left module is similarly defined, with notation ${}_R M$

- ~ The definitions for **submodule**, **quotient module**, and **simple module** are all as expected.
- ~ Given rings R, S , then ${}_R M_S$ is a **bimodule** if M is a left R -module and a right S -module, and $(rm)s = r(ms)$.
- ~ A set of elements, $\{m_\alpha\}_{\alpha \in A}$, **generates** M if for any $m \in M$, we have that $m = m_{\alpha_1}r_{\alpha_1} + \dots + m_{\alpha_n}r_{\alpha_n}$ with $r_{\alpha_j} \in R$.
- ~ A module M_R is **finitely generated** if there exists a finite set of generators for M .
- ~ M_R is a **free module** if there exists a generating set, A , such that the representation of elements of M as linear combinations of elements of B is unique.
- ~ For a module M_R , over a commutative ring R that is a PID,

$$T(M) := \{m \in M : mr = 0 \text{ for some } r \neq 0\}.$$

- ~ A module M_R for a commutative PID, R , is called **torsion free** if $T(M) = (0)$.
- ~ A module is **simple** if the only submodules are (0) and itself.
- ~ A module M_R is **cyclic** if it can be generated over R by a single element.
- ~ Given $M \triangleleft R$, then if every free R/M -module has the same number of basis elements, then we say that R/M has the **invariant basis number property (IBN)**.

~ Let M_i be R -modules, then,

$$\longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow$$

is **exact at i** if $\text{Im}(f_{i-1}) = \text{Ker}(f_i)$. The sequence is **exact** if it is exact at all i .

~ A sequence of the form $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ which is exact is called a **short exact sequence**.

~ A **split short exact sequence** is a short exact sequence such that there is a map g' such that $g \circ g' = \text{id}_C$.

~ A **linear transformation** from M_R to N_R is a function $f : M \rightarrow N$ such that $f(m_1 + m_2) = f(m_1) + f(m_2)$ and $f(mr) = f(m)r$.

~ A module, M is **complemented** if for every nonzero submodule, N , there is another submodule, N' such that $N \oplus N' = M$.

~ A nonzero submodule, $U \subset M$ is **essential** if $U \cap T \neq (0)$ for all nonzero submodules $T \subset M$.

~ A **bilinear function** is a function $f : A_R \times_R B \rightarrow G$ where G is an abelian group, and A and B are R -modules, such that the following three properties hold:

- $f(a + a', b) = f(a, b) + f(a', b)$
- $f(a, b + b') = f(a, b) + f(a, b')$
- $f(ar, b) = f(a, rb)$

where $a, a' \in A$, $b, b' \in B$ and $r \in R$.

~ A **tensor product** of A_R and ${}_R B$ is an abelian group $A \otimes_R B$ and a bilinear function, f such that there exists a unique group homomorphism $f' : A \otimes B \rightarrow G$ such that the following diagram commutes:

$$\begin{array}{ccc} A \times B & \xrightarrow{\pi} & A \otimes B \\ \downarrow f & \swarrow f' & \\ G & & \end{array}$$

3.1.3 Definitions connecting Rings and Modules

~ If for any family of submodules of M_R , \mathcal{F} , there is a maximal element in \mathcal{F} , then M_R satisfies the **maximal condition**.

~ If M_R satisfies the maximal condition, then M_R is called **Noetherian**.

~ A ring R is a **Noetherian ring** if R_R is a Noetherian module.

- ~ A module M_R satisfies the **minimal condition** if any nonempty family of submodules of M has the property that there exists a minimal element in the family.
- ~ A module, M_R is **Artinian**, if it satisfies the minimal condition.
- ~ A ring R is **Artinian** if R_R is an Artinian module.
- ~ A module N_R is **faithful** if $\text{Ann}_R(M) = \{r : mr = 0 \forall m \in M\} = (0)$.
- ~ A ring R is **primitive** if it has a faithful simple module.

3.1.4 Definitions involving Groups, Rings, and/or Fields

- ~ Let G be a finite group and F a field. the **group algebra** of G over F is written $F(G)$ and is the algebra formed in the obvious way from the obvious vector space over F with basis elements in G .
- ~ A **representation** of a group G is a homomorphism ψ of G into $GL(V)$ on a vector space V over some field. Here V is called the **representation module belonging to** ψ .
- ~ If G is a group of order p^n , and $\text{char}(F) = p$, then let $\phi : F(G) \rightarrow F$ be given by $\phi(g) = 1$ for all g , then $\ker(\phi)$ is called the **augmentation ideal** of $F(G)$. Also, $J(F(G)) = wG$ and is generated by $\{(1 - g) : g \in G\}$.
- ~ Two matrices, $A, B \in M_n(F)$ are **similar** if there exists $P \in M_n(F)$ such that $B = PAP^{-1}$.
- ~ The **minimal polynomial**, $m(x)$ of T is the monic polynomial such that $m(T) = 0$, and if $p(x)$ is another polynomial such that $p(T) = 0$, then $m(x)|p(x)$.
- ~ If A is a linear transformation $V \rightarrow V$, and $Av = \lambda v$ for $\lambda \in F$ and $v \in V$, then v is called an **eigenvector**, and λ is called an **eigenvalue**.
- ~ $\det(A - xI)$ is the **characteristic polynomial** of A . The roots of this polynomial will be the eigenvalues.

3.2 Theorems and Other Ring/Module Statements

3.2.1 Integral Domains

Remark. Every nonzero ideal is free in a PID.

Proposition. *If R is a PID, then irreducible elements are prime.*

Theorem. *If R is a PID, then R is a UFD.*

Theorem. *If R is an ED, then R is a PID.*

Proposition. *A PID is Noetherian.*

Proposition. *If R is a PID, then all nonzero prime ideals are maximal ideals.*

3.2.2 Chain Conditions, Noetherian, Artinian

Theorem. *The following are equivalent on a module M_R :*

- ~ Ascending chain condition (ACC) on submodules, if $M_1 \subset M_2 \subset \dots$ then there exists an n such that $M_i = M_n$ for all $i \geq n$.*
- ~ Any submodule is finitely generated.*
- ~ If \mathcal{F} is a family of submodules of M then there is a maximal element in \mathcal{F} . This is called the maximal condition.*

Theorem. *If R is a commutative ring with identity, and every prime ideal is finitely generated, then R is Noetherian.*

Proposition. *The minimal condition is equivalent to the descending chain condition.*

Proposition. *Submodules, factor modules, and direct sums of Noetherian modules are Noetherian.*

Corollary. *If R is right Artinian, then R is left Artinian.*

Theorem. *Given a short exact sequence $0 \leftarrow A_R \leftarrow B_R \leftarrow C_R \leftarrow 0$, if any two of A, B, C are Noetherian, then so is the third.*

Proposition. *If $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is a short exact sequence, then if any two of A, B, C are Artinian, then so is the third.*

Proposition. *Let R be a Noetherian ring. If M_R is a finitely generated R -module, then M_R is Noetherian.*

Proposition. *If R_R is right Artinian, then a finitely generated right R -module, M_R , is also Artinian*

Hilbert Basis Theorem. *If R is a Noetherian ring (need not be commutative), then $R[x]$ is also Noetherian.*

Corollary. *If R is commutative and Noetherian, then $R[x_1, \dots, x_n]$ is also Noetherian.*

Proposition. *If R is an Artinian ring, then $M_n(R)$ is also Artinian*

Hopkins' Theorem. *If R is a right Artinian ring with identity, then R is right Noetherian.*

Hopkins' Theorem. *If R is a right Artinian ring, then any nil right ideal is nilpotent. The statement also holds for left rings and ideals.*

Artin-Tate Lemma. *Let R be a commutative Noetherian ring, and let S be a ring extension of R . Then, if $T = R[a_1, \dots, a_n]$ is a finitely generated S module, then S is finitely generated as a ring over R .*

3.2.3 Modules over a PID

In this section, all rings are commutative principal ideal domains.

Theorem. *Any submodule of a free module of finite rank over a PID is also free of rank at most that of the original module.*

Proposition. *$T(M)$ is a submodule of M .*

Proposition. *$T(M/T(M)) = (0)$.*

Theorem. *Let M_R be a finitely generated torsion free module over R . Then M_R can be embedded into a finitely generated free R -module.*

Theorem. *Let R be a PID and M_R be finitely generated. Then $M = R_R \oplus S$ where $T(S) = S = T(M)$.*

Theorem. *A finitely generated torsion module over a PID is a direct sum of cyclic submodules $C_1 \oplus \dots \oplus C_t$ such that if $C_i = c_i R$, then $\text{Ann}(c_i) \subset \text{Ann}(c_{i+1})$. Also, $C_i \cong R/\text{Ann}(c_i)$, and this representation is unique..*

3.2.4 Exact Sequences

Proposition. *The sequence $0 \longrightarrow A_R \xrightarrow{f} B_R$ is exact at A if and only if f is injective.*

Proposition. *The sequence $A \xrightarrow{g} B \longrightarrow 0$ is exact at B if and only if g is surjective.*

Proposition. *A sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is exact if and only if $C \cong B/A$.*

Lemma. *If $A \xrightarrow{f} B \longrightarrow 0$ is exact and there exists a function $g : B \rightarrow A$ such that $f \circ g = \text{id}_B$, then $A = g(B) \oplus \ker(f)$.*

Corollary. *If the sequence $A \xrightarrow{f} F \longrightarrow 0$ is exact and F is free, then $A \cong F \oplus \ker(f)$.*

3.2.5 Semiprime Artinian Rings

Proposition. *Let R be a semiprime ring with identity, then if K is a minimal right ideal, we can write $K = eR$ for some idempotent e .*

Proposition. *If R is a semiprime ring, then eR is a minimal right ideal (with e an idempotent) if and only if eRe is a division ring.*

Corollary. *If R is a semiprime ring, then eR is a minimal right ideal with e an idempotent if and only if Re is a minimal left ideal.*

Proposition. *If R is a right Artinian ring, and if for any right ideal, $I^2 = (0)$ means that $I = (0)$, then any right ideal K is of the form $K = eR$ where e is an idempotent.*

Corollary. *If R is a semiprime Artinian ring, then R is right Noetherian.*

Proposition. *If R is a semiprime right Artinian ring, then any two sided ideal is generated by a central idempotent.*

Theorem. *If R is a semiprime Artinian ring, then $R = S_1 \oplus \dots \oplus S_t$ where each S_i is a simple Artinian ring. This representation is unique.*

Proposition. *If R is a semiprime Artinian ring, then every module is a sum of simple submodules.*

Remark. In this section, we did not use the fact that our semiprime Artinian rings had an identity element, but we did prove that they must have one.

3.2.6 Nilpotence

Remark. The nilpotent elements form an ideal, $N = N(R)$. Also, R/N has no nonzero nilpotent elements.

Proposition. *Let N be the ideal of nilpotent elements. Then $N = \bigcap_{i \in I} P_i$ where $\{P_i\}_{i \in I}$ is the set of all prime ideals.*

Theorem. *If R is a commutative Noetherian ring, and N is the ideal consisting of nilpotent elements, then there exists a $t \geq 1$ such that $N^t = (0)$.*

Proposition. *If $A \in M_n(F)$, and A is nilpotent, then $\text{tr}(A) = 0$.*

Wedderburn's Theorem. *If A is a finite dimensional algebra over a field K , and every element in A is a sum of nilpotent elements, then A is nilpotent.*

Theorem. *If A is a finite dimensional algebra over K , and A is nil, then A is nilpotent.*

Theorem. *If R_R is Artinian, then there exists a nilpotent two sided ideal that contains all nil one sided ideals. This ideal is called the **(nil) radical of R** .*

Corollary. *If R is Artinian, and N is the nil radical of R , then R/N is semiprime.*

Theorem. *A subring of $M_n(\Delta)$ where Δ is a division ring, that consists of nilpotent elements is nilpotent. Also, this subring can be triangularized.*

Levitsky's Theorem. *If R is a right Noetherian ring, then any nil right or left ideal is nilpotent.*

Proposition. *If T is a subring of $M_n(\Delta)$, then T contains maximal nilpotent subrings.*

Theorem. *If R is a right Artinian (or right Noetherian) ring, then any nil subring of R is nilpotent.*

3.2.7 Algebraic Geometry Introduction

Proposition. *An element $r \in J(R)$ if and only if $1 + r$ is invertible. In fact, the Jacobson Radical is the largest ideal such that $1 + x$ is invertible for every x in the ideal.*

Proposition. *If n is nilpotent, then $n \in J(R)$.*

Theorem. *If R is a homomorphic image of $K[x_1, \dots, x_n]$, then $J(R) = N(R)$.*

Classical Nullstellensatz. *If K is an algebraically closed field, then let I be an ideal of $K[x_1, \dots, x_n]$. If for the polynomial h we have that $h(c_1, \dots, c_n) = 0$ for all (c_1, \dots, c_n) that I vanishes on, then $h^t \in I$.*

Proposition. *If I is the ideal generated by a subset $S \subset K[x_1, \dots, x_n]$ with $K = \overline{K}$, then $V(I) = V(S)$.*

Proposition. *$V(K[x_1, \dots, x_n]) = \emptyset$, and $I(K^n) = (0)$*

Proposition. *If $S \subset T \subset K[x_1, \dots, x_n]$, then $V(T) \subset V(S)$. Similarly, if $A \subset B \subset K^n$, then $I(B) \subset I(A)$.*

Proposition. *If $S \subset K[x_1, \dots, x_n]$, then $I(V(S)) \supseteq S$.*

Theorem. *If K is an algebraically closed field, and J is a proper ideal of $K[x_1, \dots, x_n]$, then $\sqrt{J} = I(V(J))$ where $\sqrt{J} = \{h : h^t \in J, t \in \mathbb{N}\}$.*

3.2.8 Division Rings

Wedderburn's Theorem. *A finite division ring is a field.*

Schur's Lemma. *If M_R is simple, then $\text{End}_R(M_R)$ is a division ring.*

Proposition. *If D is a division ring that is finite dimensional over its center, and that center is algebraically closed, then it is equal to its center.*

3.2.9 Tensor Products

Theorem. *$A \otimes_R B$ exists and is unique.*

Proposition. *$A \otimes_R B \cong F/S$ where F is the free group generated by all elements (a, b) , and S is the subgroup of F generated by all elements of the form $(a + a', b) - (a, b) - (a', b)$, $(a, b + b') - (a, b) - (a, b')$, and $(ar, b) - (a, rb)$.*

Proposition. *Given homomorphisms $f : A_R \rightarrow A'_R$, and $g : {}_R B \rightarrow {}_R B'$, there is a homomorphism $f \otimes g : A \otimes_R B \rightarrow A' \otimes_R B'$ given by $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$.*

Proposition. *Given homomorphisms $A_R \xrightarrow{f} A'_R \xrightarrow{f'} A''_R$ and ${}_R B \xrightarrow{g} {}_R B' \xrightarrow{g'} {}_R B''$, then, $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$.*

Theorem. Given rings R, S , and modules A_R and ${}_R B_S$, then $A \otimes_R B$ is a right S -module via the action $(a \otimes b)s = a \otimes (bs)$.

Proposition. $R \otimes_R B \cong_R B$

Proposition. Given a commutative ring R , then $A \otimes_R B \cong B \otimes_R A$.

Proposition. Associativity of tensor product: Given rings R, S and an $R - S$ -bimodule B , then $(A \otimes_R B) \otimes_S C \cong A \otimes_R (B \otimes_S C)$.

Proposition. Distribution in tensor products: $A \otimes (\oplus_i C_i) \cong \oplus_i (A \otimes C_i)$.

Theorem. If ${}_R A \xrightarrow{f} {}_R B \xrightarrow{g} {}_R C \longrightarrow 0$ is exact, and M_R is a right R -module, then

$$M \otimes A \xrightarrow{id \otimes f} M \otimes B \xrightarrow{id \otimes g} M \otimes C \longrightarrow 0$$

is also exact.

3.2.10 Vector Spaces, Matrices, and Linear Transformations

Theorem. $A, B \in M_n(F)$ with F a field are similar if and only if the corresponding $F[x]$ -modules are isomorphic as $F[x]$ -modules.

Theorem. If $T : V_F \rightarrow V_F$ and $\dim_F(V) < \infty$, then V^T is a finitely generated torsion module over $F[x]$.

Proposition. Let $f(x) \in F[x]$ be a polynomial of degree n . Then $F[x]/(f(x))$ has a basis of the form $\{1 + (f(x)), x + (f(x)), \dots, x^{n-1} + (f(x))\}$.

Proposition. Let W be a cyclic submodule of V^T with dimension n . If w generates W , then $\{w, Tw, \dots, T^{n-1}w\}$ is a basis for W .

Theorem. Let $T \in \mathcal{L}(V, V)$ Let $\{f_1 \dots f_k\}$ be the invariant factors of T . Then $\dim(V^T) = \sum \deg(f_i)$ and $V^T = F[x]/(f_1(x)) \oplus \dots \oplus F[x]/(f_k(x))$.

Proposition. If $T, S : V \rightarrow V$, then S and T are similar matrices if and only if $V^T \cong V^S$.

Theorem. If A, B are $n \times n$ matrices with entries in a field F , then A and B are similar if and only if there is a field $K \supseteq F$ such that A and B are similar over K .

Cayley Hamilton theorem. Let $p_A(x)$ be the characteristic polynomial of A . Then $p_A(A) = 0$.

Theorem. If $A : V \rightarrow V$ is a linear transformation, and the minimal polynomial of A factors completely into linear factors over the base field, F , then there is a basis such that A is upper triangular with respect to that basis.

3.2.11 Simple Rings and Modules

Proposition. *If R is a simple Artinian ring, then $R \cong \text{End}_{eRe}(eR)$.*

Corollary. *If R is a simple Artinian ring, then $R \cong D_n$ where D_n is $n \times n$ matrices over a division ring D .*

Lemma. *If M is a complemented module, then every submodule contains a simple submodule.*

Theorem. *M is a complemented module if and only if M is equal to the direct sum of simple submodules.*

Proposition. *If a module is simple, then it is also cyclic.*

Proposition. *If R is any simple ring with a minimal right ideal, I , then all simple R modules are isomorphic.*

Proposition. *Given M , a simple R -module, and $\phi : R \rightarrow M$ given by $\phi(r) = mr$, then ϕ is a module homomorphism, and $M \cong R/\ker(\phi)$, and so $\ker(\phi)$ is a maximal right ideal of R . In other words, every simple R -module is of the form M/K where K is a maximal right ideal of R . Conversely, if K is a maximal right ideal of R , then R/K is a simple R -module.*

3.2.12 Prime, Primitive and Maximal: Rings, Ideals, and Elements

Theorem. *If P is an ideal in a ring R such that $P \neq R$ and for all $a, b \in R$ we have that $ab \in P$ means that $a \in P$ or $b \in P$, then P is a prime ideal. If R is also commutative, then the reverse statement holds.*

Remark. Prime elements are always irreducible.

Lemma. *If Q is an ideal that is maximal with respect to exclusion of a multiplicatively closed subset S of R , then Q is prime.*

Theorem. *The maximal ideals of $\mathbb{C}[x_1, \dots, x_n]$ are of the form $((x_1 - a_1), \dots, (x_n - a_n))$ with $a_1, \dots, a_n \in \mathbb{C}$.*

Corollary. *If M is a maximal ideal in $\mathbb{Z}[x_1, \dots, x_n]$, then $M \cap \mathbb{Z} \neq (0)$.*

Proposition. *If R is a primitive ring, and $0 \neq I, J \triangleleft R$ (two sided), then if $IJ = (0)$, we have that either $I = (0)$, or $J = (0)$.*

Proposition. *Every primitive ring is prime, but not all prime rings are primitive.*

Proposition. *A ring R is prime if and only if the product of nonzero right (or left) ideals is nonzero.*

3.2.13 Group Algebras

Remark. If A is a ring that is also a vector space over K , then A is an algebra over K if $\alpha(a_1a_2) = (\alpha a_1)a_2 = a_1(\alpha a_2)$ for $a_1, a_2 \in A$.

Maschke's Theorem. *If G is a finite group, then $F(G)$ is semisimple if and only if $\text{char}(F) \nmid |G|$.*

Proposition. *If A is a finite dimensional simple algebra over an algebraically closed field, K , then $A \cong M_n(K)$.*

Proposition. *wG is a finite dimensional vector space over F .*

Proposition. *$F(G)/wG \cong F$.*

3.2.14 Miscellaneous

Proposition. *If F_R is a free module with basis I , then*

$$F_R \cong \bigoplus_{i \in I} R.$$

Theorem. *If a commutative ring R has an ideal M , such that R/M has IBN, then so does R .*

Proposition. *$R \oplus R / (R \oplus R)M \cong R/M \oplus R/M$.*

Proposition. *Let M_R be a module, and $S = \text{End}_R(M)$. Then M is an S - R -bimodule. Moreover, W is a T - U -bimodule if and only if $T \subset \text{End}_U(W)$.*

Proposition. *Let R be a ring with identity, and M an R -module. Then $\text{End}_R(\bigoplus_{i=1}^n M) \cong (\text{End}_R(M))_{n \times n \text{ matrices}}$. Similarly, if F is a field, then $\text{End}_F(\bigoplus_{i=1}^n F) \cong M_n(F)$.*